IN THE UNITED STATES DISTRICT COURT FOR THE
WESTERN DISTRICT OF MISSOURI
WESTERN DIVISION

**UNITED STATES OF AMERICA,**

Plaintiff,

v.

**(1) JOSEPH A. CAMP,**
[DOB: 05/28/84]

and

**(2) DANIEL J. FOWLER,**
[DOB: 08/07/89]

Defendants.

No. _____

**COUNT ONE:**
**18 U.S.C. § 371**
**(Conspiracy)**
NMT: 5 years
NMT: $250,000
NMT: 3 Years Supervised Release
Class D Felony

**COUNT TWO:**
**18 U.S.C. § 1030(a)(5)**
**(Computer Intrusion Causing Damage)**
NMT: 10 years
NMT: $250,000
NMT: 3 Years Supervised Release
Class C Felony

**COUNT THREE:**
**18 U.S.C. § 2511(1)(a) and (2)**
**(Interception of Electronic Communications)**
NMT: 5 Years
NMT: $250,000
NMT: 3 Years Supervised Release
Class D Felony

**COUNT FOUR:**
**18 U.S.C. § 1030(a)(4)**
**(Computer Intrusion Furthering Fraud)**
NMT: 5 Years
NMT: $250,000
NMT: 3 Years Supervised Release
Class D Felony

**COUNTS FIVE and SEVEN:**
**18 U.S.C. § 1028A(a)(1)**
**(Aggravated Identity Theft)**
2 Years Imprisonment (Mandatory)
NMT: $250,000
NMT: 3 Years Supervised Release
Class E Felony

| | | |
|---|---|---|
| | ) | **COUNT SIX:** |
| | ) | **18 U.S.C. § 1030(a)(2)** |
| **Defendants/Counts:** | ) | **(Computer Intrusion Obtaining** |
| | ) | **Information)** |
| JOSEPH CAMP - ALL COUNTS | ) | NMT: 5 years |
| DANIEL FOWLER - ALL COUNTS | ) | NMT: $250,000 |
| | ) | NMT: 3 Years Supervised Release |
| | ) | Class D Felony |
| | ) | |
| | ) | $100 Mandatory Special Assessment |
| | ) | (Each Count) |

# INDICTMENT

**THE GRAND JURY CHARGES:**

## GENERAL ALLEGATIONS

At all times relevant to this Indictment:

### Introduction

1. Between on or about March 1, 2009, and continuing thereafter to on or about March 1, 2010, in the Western District of Missouri and elsewhere, defendants JOSEPH A. CAMP and DANIEL J. FOWLER, and other persons known and unknown to the Grand Jury, engaged in an unlawful computer hacking scheme designed to gain unauthorized access to, or exceed their authorized access to, the University of Central Missouri (hereafter "UCM") computer network, and in so doing committed multiple federal criminal offenses, including Conspiracy, in violation of 18 U.S.C. § 371, Computer Intrusion, in violation of 18 U.S.C. § 1030, Aggravated Identity Theft, in violation of 18 U.S.C. § 1028A, and Interception of Electronic Communications, in violation of 18 U.S.C. § 2511.

2. In the Fall semester of 2009, CAMP and FOWLER were both students at UCM. They worked together to execute a computer hacking scheme, through which they sought to gain and use unlawful and unauthorized access to the UCM computer network to exploit the UCM and its students in several ways. The defendants obtained, or attempted to obtain, access to portions of the computer network which would allow them to change grades, view and download large databases of faculty, staff, alumni and student information, and transfer money to their student accounts. The defendants additionally sought to profit from these computer intrusions by attempting to sell lists of faculty, staff, alumni and student personal information to others.

3. The defendants accomplished the goals of this conspiracy through several unlawful methods. The defendants developed a computer virus, which they used to infect, and attempt to infect, computers used by multiple UCM faculty, staff, and students, including an attempt to infect the computer used by the UCM president. In an attempt to gain access to a computer, the defendants employed several pretexts, such as a desire to show photographs from a vacation that were contained on a thumb drive. Once they gained access, the defendants manually installed the virus. They also manually installed the virus on several UCM computers in public areas of the University, such as computer labs and the library. The defendants also attempted to send out emails to faculty and staff members of UCM with the virus hidden in an email attachment.

4. Once the defendants successfully installed this virus on a victim computer, the defendants obtained remote access to the victim computer, which allowed them to capture keystrokes of the user, download any of that user's files, and remotely turn on that user's webcam to watch and photograph the user of the victim computer. The defendants did this in an attempt

to gain the personal information of these UCM faculty, staff, and students, as well as gain their access rights to the UCM network for further exploits.

5. The defendants successfully distracted and misled at least one UCM administrator and were able to use a thumb drive to download their virus onto his UCM computer. The defendants then used this virus to monitor this administrator's computer activity and capture the administrator's username and password. The defendants also used their remote access of this administrator's computer to remotely turn on this administrator's webcam to watch and photograph this administrator sitting at his desk in his office. The defendants also downloaded and obtained his emails.

6. The defendants successfully used the identity of at least one residence hall director to further their computer hacking scheme. By unlawfully obtaining the username and password of a residence hall director, and then using this residence hall director's access to the UCM network, the defendants were able to exploit the UCM computer system by conducting, and attempting to conduct, financial transactions, in an attempt to unlawfully credit their student accounts with UCM funds.

7. The defendants successfully used the identities of fellow students to accomplish the goals of the conspiracy. Without authorization, the defendants used the identity and University computer network permissions of other students, to gain access to various portions of the computer network they would otherwise not have access to, which enabled them to mask their activities, and mislead University authorities to the identities of those conducting the attacks on the computer network.

8. When their activities were discovered by law enforcement, the defendants also used the social media website Facebook.com to communicate threats and harass potential witnesses against them.

9. At all times relevant to this Indictment, the University of Central Missouri (UCM) was a public institution of higher learning located in Warrensburg, Missouri, within the Western District of Missouri, and it was engaged in interstate and foreign commerce.

10. During the UCM fall semester of 2009, CAMP and FOWLER were enrolled as students at UCM, and possessed the normal student access rights to the UCM computer network, as stated in the UCM student policy handbook. Additionally, FOWLER also served as a Community Advisor with University housing. At all times relevant to this Indictment, CAMP and FOWLER did not have permission to possess or use the UCM login and password information of UCM administrator E.S., UCM residence hall director M.K., and UCM student, J.B.

## COUNT ONE
**(Conspiracy)**

11. The General Allegations set forth in paragraphs One through Ten of this Indictment are re-alleged as if stated fully here.

12. Between on or about March 1, 2009, and continuing thereafter to on or about March 1, 2010, within the Western District of Missouri and elsewhere, JOSEPH A. CAMP, and DANIEL J. FOWLER, and other persons both known and unknown to the Grand Jury, did knowingly and intentionally combine, conspire, confederate, and agree with one another to:

a. Knowingly cause the transmission of a program, information, code, and command, and as a result of such conduct, intentionally cause damage without

authorization, to a protected computer, and cause loss during a one-year period aggregating at least $5,000 in value, in violation of Title 18, United States Code, Sections 1030(a)(5)(A)(i), 1030(a)(5)(B)(i), and 1030(c)(4)(A);

b. Knowingly and intentionally intercept, and endeavor to intercept, certain wire and electronic communications, to wit: electronic mail messages (emails), computer keystrokes, and video and still images, of others without the knowledge or consent of said individuals, and such wire and electronic communications were sent through a system or systems that affect interstate or foreign commerce, in violation of Title 18, United States Code, Sections 2511(1)(a) and (4)(a), and 2;

c. Knowingly and with the intent to defraud, access a computer without authorization and in excess of their authorization, and by means of such conduct furthered the intended fraud and attempted to obtain something of value, specifically, United States Currency, and the value of such use was more than $5,000 within a 1-year time period, in violation of Title 18, United States Code, Sections 1030(a)(4), 1030(b), and 1030(c)(3)(A); and,

d. Intentionally access a computer without authorization and in excess of their authorization, and thereby obtained information from a protected computer, to wit: databases containing faculty, staff, alumni, and student identification information, each of which is a computer involved with interstate or foreign communication, and the offense was committed for commercial advantage or private financial gain, in violation of Title 18, United States Code, Sections 1030(a)(2), 1030(b) and 1030(c)(2)(B)(i).

## THE OBJECT OF THE CONSPIRACY

13. The object of the unlawful computer hacking conspiracy was to gain unauthorized access, or exceed authorized access to, information and computer network resources at the UCM, for the purpose of monitoring faculty and staff members, changing grades, stealing money, and stealing faculty, staff, alumni, and student identification information to sell for profit.

## MANNER AND MEANS OF THE CONSPIRACY

14. The defendants employed several means to accomplish the common goal of gaining unlawful access to the UCM computer network, including but not limited to the following:

a. It was part of the conspiracy that its members would and did develop malicious software, or obtain malicious software, which could be used to capture the keystrokes and other activity of a computer user and take remote access and control of that computer user's computer;

b. It was part of the conspiracy that its members would and did distract and mislead, and attempt to distract and mislead, members of the faculty and staff of the UCM to obtain access to their computers to infect their computers with the malicious software to monitor their activity;

c. It was part of the conspiracy that its members would and did send email messages with malicious attachments to members of the faculty and staff of the UCM, and that these attachments contained the malicious code that could be used to monitor the faculty or staff member's activity on their computers;

d. It was part of the conspiracy that its members would and did use this malicious software to monitor faculty, staff, and students at the UCM, and capture their personal information, including their username login and password;

e. It was part of the conspiracy that its members would and did use their remote access and control of an administrator's computer to remotely turn on the administrator's webcam and photograph and otherwise watch the administrator at his computer;

f. It was part of the conspiracy that its members would and did use a residence hall director's username and password to obtain access to student information and make transfers of University funds;

g. It was part of the conspiracy that its members would and did use other students' identification information, including username and passwords, to mask their unlawful activity from University authorities;

h. It was part of the conspiracy that its members would and did use, and attempt to use, their unlawful access to computer network resources to conduct unauthorized financial transactions within UCM's computer network;

i. It was part of the conspiracy that its members would and did use their unlawful access to computer network resources to attempt to change or otherwise alter students' grades;

j. It was part of the conspiracy that its members would and did use their unlawful access to computer network resources to view, access, and download or otherwise copy large databases of faculty, staff, student, and alumni's personal identification information; and

k. It was part of the conspiracy that its members would and did attempt to sell large databases of faculty, staff, student, and alumni's personal identification information.

**OVERT ACTS**

15. In furtherance of the conspiracy, and to accomplish the objects of the conspiracy, one or more members of the conspiracy committed and caused to be committed various overt acts within the Western District of Missouri and elsewhere, including, but not limited to, the following:

***Using a Computer Virus to Cause Damage and Intercept Electronic Communications***

16. In or about July, 2009, FOWLER infected a computer used by K.H., a UCM student, with a computer virus which could be used to take remote access of her computer, as well as capture electronic communications, including emails, keystrokes, video and still images from her computer.

17. In or about July, 2009, CAMP, through updates from FOWLER, monitored K.H.'s activity on her computer.

18. In or about October, 2009, CAMP and FOWLER met to further develop and improve their computer virus. They developed a version of the virus that could be placed on a thumb drive, which could infect a victim-computer by connecting to the victim-computer through

its USB port. They also attempted to develop a version of the virus that could be masked behind another document, which then could be delivered via email to an unwary email recipient.

19. In or about October, 2009, CAMP and FOWLER established FOWLER's room on the UCM campus as their base of computer operations. All of the computers infected by their virus were configured to send information to computers in FOWLER's room.

20. In or about November, 2009, CAMP and FOWLER sent emails to several UCM faculty and staff members which had this computer virus attached to them, hidden within an attachment to the email.

21. In or about November, 2009, CAMP and FOWLER infected computers in public areas, including computers in the library and several computer labs on the UCM campus with the computer virus.

22. On or about October 24, 2009, CAMP discussed with K.H. the development of the virus and their plan to infect a professor's computer in order to enable them to change grades, telling her, "I only need to be on her machine for 5 minutes during installation."

23. On or about October 30, 2009, CAMP updated K.H. on the progress developing the virus, and explained, "I can get the logs sent to my email now, no need to leave a USB behind!"

24. In or about November, 2009, CAMP and K.H. visited the office of C.H., a professor at UCM, and attempted to gain access to C.H.'s computer or C.H's secretary's computer to install the virus. During this attempt, CAMP told the professor's staff members that he had pictures he wanted to show them and the pictures were on a thumb drive. A staff member offered to let CAMP show the pictures to her on her own personal computer. CAMP declined,

and pointed to C.H.'s secretary's computer and asked to use that computer. When told he could not, CAMP asked for access to C.H.'s office to "surprise" her with photos of K.H., because they were "friends." C.H.'s staff did not allow CAMP access to C.H.'s computer.

25. In or about November, 2009, CAMP and FOWLER infected a UCM administrator, E.S., with their computer virus.

26. On or about November 9, 2009, CAMP sent an email to FOWLER stating, "I wont use it anymore! Is it currently good! I assume that it was late in the day so the target was prob[ably] either on her way out or all ready gone! tomorrow morning for that email to reach its for now consider it done! Did we get a ping on that? Advise?"

27. On or about November 9, 2009, FOWLER replied in an email to CAMP stating, "I'll have the new one built by tomorrow, and I'm only in class for an hour so I should be able to keep an eye on it. You gonna hit up that one guy tomorrow? That's fine to use mine on his pc too."

28. On or about November 9, 2009, CAMP sent an email to FOWLER stating, "yeah I will sto[p] by that guys office tomorrow and talk to him!"

29. In or about November, 2009, CAMP, FOWLER, and K.H. visited E.S. at his office on the UCM campus. They convinced E.S. to give them access to his computer by stating they had photographs to show him on a thumb drive. E.S. allowed CAMP to sit at his computer, and CAMP used a thumb drive to download the computer virus onto E.S.'s computer.

30. On or about November 12, 2009, CAMP and FOWLER also attempted to download their virus onto a computer used within the office of the President of UCM. CAMP, FOWLER, and K.H. went to the office of the president of UCM. CAMP handed a thumb drive

to the administrative assistant to the president of UCM, and told her the thumb drive contained documents from his attorney that CAMP wanted the president to see, and CAMP instructed the administrative assistant to put the thumb drive into her computer. The administrative assistant declined, and handed the thumb drive back to CAMP. This thumb drive contained the computer virus developed by CAMP and FOWLER.

31. On or about November 13, 2009, CAMP sent a message to FOWLER stating, "Nice work with [E.S.]! when can [K.H.] and I stop by to check out the latest in developments? [K.H.] gets out of cls at 1 we can b there soon after," to which FOWLER replied, "That'll work"

32. On or about November 13, 2009, CAMP sent a message to FOWLER stating, "Let me know when you are back in your room! We will head over, i am really excited about [E.S.] coming bk online! I want to c his email!"

33. In or about November, 2009, CAMP and FOWLER used their remote access to E.S.'s computer to obtain his UCM computer network username and password.

34. In or about November, 2009, CAMP and FOWLER used their remote access to E.S.'s computer to turn on his webcam and monitor and photograph him at his desk.

35. In or about November, 2009, CAMP and FOWLER used their remote access to E.S.'s computer to read and download E.S.'s emails.

***Unauthorized Transfer, and Attempted Transfer, of UCM Funds***

36. On or about November 20, 2009, CAMP using the UCM computer network username and password of residence hall director M.K. attempted to conduct the following financial transactions:

| Transaction | To/(From) UCM Amount | Student Account |
|---|---|---|
| a | ($3,260) | J.B. |
| b | $3,260 | J.B. |
| c | $1,100 | J.B. |
| d | ($4,360) | J.B. |
| e | ($600) | CAMP |
| f | ($600) | CAMP |
| g | ($500) | CAMP |
| h | ($50) | CAMP |
| i | ($500) | CAMP |

37. On or about November 23, 2009, CAMP using the UCM computer network username and password of residence hall director M.K. attempted to conduct the following financial transactions:

| Transaction | To/(From) UCM Amount | Student Account |
|---|---|---|
| a | ($4,360) | J.B. |
| b | ($1,100) | J.B. |
| c | ($1,100) | J.B. |
| d | ($2,060) | J.B. |
| e | ($75) | J.B. |
| f | ($25) | J.B. |
| g | ($1,100) | CAMP |
| h | ($987.18) | CAMP |
| i | ($112.82) | CAMP |
| j | ($907.25) | CAMP |
| k | ($50) | CAMP |

| | | |
|---|---|---|
| l | ($500) | CAMP |
| m | ($25) | CAMP |
| n | ($25) | CAMP |
| o | ($1,708.92) | CAMP |
| p | ($600) | CAMP |
| q | ($1,100) | CAMP |
| r | ($1,394.30) | CAMP |
| s | ($907.25) | CAMP |
| t | ($1,100) | CAMP |
| u | ($2,060) | CAMP |
| v | ($75) | CAMP |
| w | ($25) | CAMP |

38. On or about November 23, 2009, CAMP explained to K.H. in a chat that he was using J.B.'s identity in order to conceal his actions from authorities as well as conducting the hack over Thanksgiving break in order to avoid detection, he stated, "that will all be traced back to the [J.B.] account! but the university F.S. dosn't open for the break so they will have A LOT of stuff to sort through when the semester opens, in the mean time I want direct deposit of my return! lol!"

39. On or about November 23, 2009, CAMP and K.H. were monitoring these unauthorized financial transactions to make sure they were going to go through, and CAMP told K.H. in a chat, "one last thing, I am going to show you the last 10 transactions on my account...that's how much they owe me!" Camp went on to say, "they don't want to fuck with jojo!"

40. On or about November 24, 2009, CAMP continued to access the UCM computer network to monitor these transactions, and chatted with K.H. and stated, "Remember yesterday my balance was 13000 and change?" K.H. replied, "wow, yes I see!" CAMP stated, "whos a bawse?"

41. On or about November 25, 2009, CAMP was arrested by the UCM police department. CAMP possessed the username and password for J.B. written on a piece of paper in his pants pocket.

42. On or about November 25, 2009, CAMP's computers were seized by the UCM police department. On his computers, CAMP possessed the username and password for M.K. and E.S.

43. On or about November 25, 2009, CAMP also possessed the keylogging programs Spector Pro and Poison Ivy on his computers.

***Unlawful Possession and Attempted Sale of UCM Faculty, Staff, Alumni and Student Information***

44. In or about December, 2009, CAMP and FOWLER unlawfully possessed UCM databases containing faculty, staff, alumni, and student information.

45. In or about December, 2009, CAMP contacted T.S. and informed T.S. in a recorded call that he had personal information of thousands of people that he and FOWLER obtained from UCM, and that they wanted to sell the information.

46. In or about December, 2009, CAMP told T.S. in a recorded call that UCM would not do anything to him for the hack over Thanksgiving, because if they did, he would embarrass them publically and the University would not want all of the bad publicity.

47. In or about December, 2009, CAMP told T.S. in a recorded call about all of the access he and FOWLER had to the UCM computer system, and that they could do anything they wanted. CAMP told T.S., "the cops were dumb to bust us so quick" and "if they knew the scope of this, they would have involved the feds."

48. In or about December, 2009, CAMP and FOWLER created four Microsoft Excel spreadsheets which contained personal information of UCM faculty, staff, alumni, and students to sell to T.S.

49. In or about December, 2009, CAMP asked T.S. in a recorded call to find a buyer for the lists of UCM information, which CAMP and FOWLER would sell to the buyer, and give T.S. a share.

50. In or about December, 2009, CAMP traveled to New York to meet T.S. to sell the lists of UCM personal information to the buyer that T.S. had arranged.

51. On or about December 23, 2009, CAMP and FOWLER communicated via text messages regarding the sale of the UCM lists, and during the attempted sale itself about whether or not CAMP should complete the sale. Prior to the attempted sale of the lists, FOWLER sent CAMP a text message which read, "Checking. I'll send 'leave' if its bad. otherwise nothing."

52. On or about December 23, 2009, CAMP met with T.S. and U.C. and showed U.C. samples of the lists of UCM information. CAMP told U.C. he would sell him 90,000 identities for $35,000.

53. On or about December 23, 2009, CAMP was arrested for attempting to sell the four lists of personal information of UCM faculty, staff, alumni, and students, and had the lists on computers in his possession.

54. After his arrest, CAMP told K.H. in a recorded call to, "Tell D that he [CAMP] is in jail and that the FBI has the lists."

***Witness Tampering and Destruction of Evidence***

55. Between on or about November 25, 2009, and on or about December 4, 2009, CAMP and FOWLER obtained a copy of the affidavit used to obtain a search warrant for CAMP's room at UCM.

56. On or about December 4, 2009, CAMP posted an excerpt from the affidavit on his Facebook.com page. In addition to the excerpt from the affidavit, CAMP said, "I am very concerned about anyone who lies to the police! Think I don't know? I have the papers now! I KNOW WHOs THE SNITCH!". CAMP also posted, "I really hope you are feeling like shit for getting your friends in trouble...Since this is bound for trial I really hope that you plan to be around...and then suffer the media attention...and then the embarras[s]ment that you lied and ratted on someone..."

57. On or about December 5, 2009, CAMP posted on his Facebook.com page, "I am not a fan of people who lie to the police to get other innocent people in trouble. I will make it a point to post anything that I find out here on facebook so that you feel ashamed about l[y]ing to the police. I wont reda[ct] anything. I will MAKE SURE that your name is posted with the lies you told!"

58. In or about December, 2009, CAMP told T.S. in a recorded call that he posted this on Facebook, "to scare the girl that talked."

59. On or about December 30, 2009, just days after CAMP's arrest in New York, UCM police executed a search warrant on FOWLER's UCM dorm room. All of the computers

had been removed from the room. UCM detectives found a post-it on a remaining computer monitor which read, "too late!" with a smiley face on it.

***Substantive Counts***

60. The facts of each of the separate offenses charged in Counts Two through Four, and Six are alleged to be separate overt acts undertaken in furtherance of the conspiracy and to accomplish one or more objects of the conspiracy, and are incorporated by reference as if fully set forth herein as separate overt acts.

61. All in violation of Title 18, United States Code, Section 371.

**COUNT TWO**
**(Computer Intrusion Causing Damage)**

62. The General Allegations set forth in paragraphs One through Ten of this Indictment are re-alleged as if stated fully here.

63. Between on or about October, 2009, and on or about December, 2009, in the Western District of Missouri and elsewhere, JOSEPH A. CAMP and DANIEL J. FOWLER, and others both known and unknown to the Grand Jury, aiding and abetting each other and others, without authorization, knowingly caused the transmission of a program, information, code and command, and as a result of such conduct, intentionally caused damage to a protected computer, and the offense caused loss to persons during a 1-year period from the defendants' course of conduct affecting protected computers aggregating at least $5,000 in value.

64. All in violation of Title 18, United States Code, Sections 1030(a)(5)(A), 1030(b), and 1030(c)(4)(B) and 2.

**COUNT THREE**
**(Interception of Electronic Communications)**

65. The General Allegations set forth in paragraphs One through Ten of this Indictment are re-alleged as if stated fully here.

66. Between on or about October, 2009, and on or about December, 2009, in the Western District of Missouri and elsewhere, JOSEPH A. CAMP and DANIEL J. FOWLER, and others both known and unknown to the Grand Jury, aiding and abetting each other and others, knowingly and intentionally intercepted and endeavored to intercept certain wire and electronic communications, to wit: electronic mail messages (emails), computer keystrokes, and video and still images, of others without the knowledge or consent of said individuals, and such wire and electronic communications were sent through a system or systems that affect interstate and foreign commerce.

67. All in violation of Title 18, United States Code, Sections 2511(1)(a) and (4)(a), and 2.

**COUNT FOUR**
**(Computer Intrusion Furthering Fraud)**

68. The General Allegations set forth in paragraphs One through Ten of this Indictment are re-alleged as if stated fully here.

69. Between on or about November 20, 2009, and on or about November 23, 2009, in the Western District of Missouri and elsewhere, JOSEPH A. CAMP and DANIEL J. FOWLER, and others both known and unknown to the Grand Jury, aiding and abetting each other and others, knowingly and with the intent to defraud, accessed a computer without authorization and in excess of their authorization, and by means of such conduct furthered the intended fraud and

attempted to obtain something of value, specifically, United States Currency, and the value of such use was more than $5,000 within a 1-year time period.

70. All in violation of Title 18, United States Code, Sections 1030(a)(4), 1030(b), 1030(c)(3)(A) and 2.

**COUNT FIVE**
**(Aggravated Identity Theft)**

71. Between on or about November 20, 2009, and on or about November 23, 2009, in the Western District of Missouri and elsewhere, JOSEPH A. CAMP and DANIEL J. FOWLER, and others both known and unknown to the Grand Jury, aiding and abetting each other and others, did knowingly possess and use, without lawful authority, a means of identification of another person, namely login credentials of a staff member and student, including his University computer network login username and password, during and in relation to an offense under 18 U.S.C. § 1030(a)(4), namely Computer Intrusion Furthering Fraud as described in Count Four, and incorporated by reference, an offense enumerated under 18 U.S.C. § 1028A(c)(4).

72. All in violation of Title 18, United States Code, Sections 1028A and 2.

**COUNT SIX**
**(Computer Intrusion Obtaining Information)**

73. The General Allegations set forth in paragraphs One through Ten of this Indictment are re-alleged as if stated fully here.

74. Between on or about October, 2009, and on or about December, 2009, in the Western District of Missouri and elsewhere, JOSEPH A. CAMP and DANIEL J. FOWLER, and others both known and unknown to the Grand Jury, aiding and abetting each other and others, intentionally accessed a computer without authorization and in excess of their authorization, and

thereby obtained information from a protected computer, to wit: databases containing faculty, staff, alumni and student personal identification information, each of which is a computer involved with interstate or foreign communication, and the offense was committed for commercial advantage or private financial gain;

75. All in violation of Title 18, United States Code, Sections 1030(a)(2), 1030(b), 1030(c)(2)(B)(i) and 2.

**COUNT SEVEN**
**(Aggravated Identity Theft)**

76. Between on or about October, 2009, and on or about December, 2009, in the Western District of Missouri and elsewhere, JOSEPH A. CAMP and DANIEL J. FOWLER, and others both known and unknown to the Grand Jury, aiding and abetting each other and others, did knowingly possess and use, without lawful authority, a means of identification of another person, namely login credentials of a faculty and staff member, including their University computer network login usernames and passwords, during and in relation to an offense under 18 U.S.C. § 1030(a)(2), namely Computer Intrusion Obtaining Information as described in Count Six, and incorporated by reference, an offense enumerated under 18 U.S.C. § 1028A(c)(4).

77. All in violation of Title 18, United States Code, Sections 1028A and 2.

A TRUE BILL.

/s/ Micheal R. Bailey
FOREPERSON OF THE GRAND JURY

/s/ Matthew P. Wolesky
Matthew P. Wolesky, #53253
Assistant United States Attorney

DATED: 11/18/10

**JS 45 (1/96)**

UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF MISSOURI

**CRIMINAL CASE COVER SHEET**

**Division of Filing**
☒ Western ☐ St. Joseph
☐ Central ☐ Southern
☐ Southwestern

**Place of Offense**
Jackson County

**Matter to be Sealed**
☐ Secret Indictment
☐ Juvenile

**Defendant Information**
Defendant Name Joseph A. Camp
Alias Name
Birthdate 05/28/1984

**Related Case Information**
Superseding Indictment/Information ☐Yes ☐No
if yes, original case number _____

New Defendant ☒Yes ☐No
Prior Complaint Case Number, if any _____

**U.S. Attorney Information**
AUSA Matthew P. Wolesky

**Interpreter Needed**
☐ Yes Language and/or dialect _____
☒ No

**Location Status**
Arrest Date ___
☒ Currently in Federal Custody
☐ Currently in State Custody Writ Required ☐ Yes ☐ No
☐ Currently on bond

**U.S.C. Citations**
Total # of Counts 7

| Set | Index Key/Code/Offense Level | Description of Offense Charged | Count(s) |
|---|---|---|---|
| 1 | 18:371.F/4992/4 | Conspiracy to Defraud the United States | 1 |
| 2 | 18:1030A.F/4996/4 | Fraud Activity Connected with Computers | 2, 4,6 |
| 3 | 18:2511.F/9911/4 | Interception and Disclosure of Wire or Oral Communications | 3 |

(May be continued on reverse)

**Date** 11/18/2010 **Signature of AUSA** */s/ Matthew P. Wolesky*

| Set | Index Key/Code/Offense Level | Description of Offense Charged | Count(s) |
|---|---|---|---|
| 4 | 18:1028A.F/4991/4 | raud with Identification Documents | 5, 7 |
| 5 | | | |